Fault Tolerant Schemes in ARGOS

Pure Software Methods in ARGOS
- Algorithm Based Fault Tolerance
- Stutter Step Mode
- Assertions
- Control Flow Checking
- Watchdog Task

Algorithm Based Fault Tolerance for FFT
- \( X = A_n \cdot x \)
- \( rw = (W_3^{BR(0)}, W_3^{BR(1)}, ..., W_3^{BR(N-1)}) \)
- \( ws = rw \cdot^* An \)
- \( X(N) = ws \cdot x' = (rw \cdot^* An) \cdot x' = rw' \cdot(An \cdot x') = rw'X' \)

Algorithm Based Fault Tolerance for Matrix
- The Checksum Approach
  - \( Ar = [ A \ Ae ] \)
  - \( e = [1, 1, ..., 1]^T \)
  - compare \( \text{Sum}_{over j} (a_{i,j}) ?= (Ae) \)
- \((n+1) \times (n+1)\) matrix
  - \( Af = \begin{pmatrix} A & Ae \\ e^*A & e^*Ae \end{pmatrix} \)
Stutter Step Mode

- Sequential
  
  ```
  a = fft();
b = fft();
if (a != b) error();
  ```

- Parallel (Multitasking)

Control Flow Error Detection

- Basic Block
- Interblock control flow checking
- Intrablock control flow checking

Basic Signature Monitoring

- Basic Block
- Branch-in-basic-block
- Program graph

Control Flow Checking by Signature Monitoring

- Assigned Signature
  - Structural Integrity Checking
- Derived Signature
  - Signatured Instruction Streams
  - Branch Address Hashing
  - Path Signature Analysis
  - Continuous Signature Monitoring
  - Extended Precision Checksum

Signature Analysis by Instructions

- Assigned Signature Analysis
- No extra hardware
- Interblock control flow checking
- Signature comparison by instructions instead of hardware

Preliminaries

- Basic Block
- Branch-in-basic-block
- Program graph
Signature Analysis by Instructions
1. Define a global variable (register) “GSR”
2. At the end of the basic block (BB), assign an arbitrary signature to GSR
3. At the head of BB, XOR GSR with the same signature above
4. If the result is not zero, an error has occurred

The detection of an error

The changes of the GSR in time

An undetected illegal branch

The DSR to detect an illegal branch

Erroneous jump to the inside
Fault Tolerant Schemes in ARGOS

Subroutine

Overhead Reduction
Combined GSR

Example

Errors with low probability (1)

Errors with low probability (2)

- The chance of missing the illegal branch in the previous slide:
  \[ P = \frac{1}{N} \]
  ( \( N \) is the \# of instructions in the scope of the conditional branch)

- The same signature in \( m \) basic blocks:
  \[ P = \frac{m}{N} \]

Reduction in if-then-else
Fault Tolerant Schemes in ARGOS

Summary
- Signature Analysis by Instructions
- Assigned Signature Analysis
- No extra hardware
- Interblock control flow checking
- Signature comparison by instructions instead of hardware